

IT INVESTMENT MANAGEMENT - EVALUATE PHASE (3.0)  
OPERATIONS AND MAINTENANCE STAGE (3.1)

Number	Phase/Stage/Task	Process Description
3.1	Operations and Maintenance Stage	<p><b>Entrance Criteria:</b> <i>The Operations/Maintenance Stage Entrance criteria is receipt by the User Representative of a signed <b>Operational Readiness Review Memorandum</b> from the System Owner(Project Sponsor).</i></p> <p><b>Purpose:</b> <i>The purpose of this stage is to collect system statistics so that IT resources and performance can be well managed and evaluated. In this stage, the system is continually monitored for performance, outages, maintenance activities, costs, resource allocation, defects, problems, and system changes. System stability is also periodically evaluated.</i></p> <p><b>Exit criteria:</b> <i>While the system is in Operations and Maintenance, it remains in the Evaluate Phase during which all stages are repeated periodically or on demand.</i></p>
		<b>Decision (Go/No Go) Points:</b>
		<b>Deliverables:</b>
		<b>Time Frames:</b>
		<p><b>Who's Involved:</b> <i>System Owner, User Representative, O&amp;M site representative, IMG, Users, System Security Specialist and the ITIB.</i></p>
		<p><b>References:</b></p> <p><i>IT Investment Management Process , Version Control Number 1.0, September 21, 2001</i></p> <p><i>Washington Office Instruction Memorandum No 2000-76 and 2000-76, Change 1</i></p> <p><i>Clearinghouse web site : <a href="http://web.blm.gov/internal/wo-500/clearinghouse.htm">http://web.blm.gov/internal/wo-500/clearinghouse.htm</a></i></p>

Number	Phase/Stage/Task	Process Description
3.1.1	User Representative monitors system performance	<b>Purpose:</b> <i>Performance and capacity management activities, performed by the O&amp;M site representative, are continually conducted while the project / system is in production. These activities include hardware and software performance monitoring and capacity planning. Statistics are generated to track system performance, utilization, and resource allocations. Actual performance is compared to performance projections made during the Select and Control Phase.</i>
		<b>Deliverables:</b>
		<b>Time Frames:</b>
		<b>Who's Involved:</b> <i>User Representative and O&amp;M site representative</i>
3.1.2	System Owner and User Representative assure Continuity of Operations	<b>Purpose:</b> <i>Assuring continuity of operations is a collection of four activities designed to manage and maintain an effective IT environment. These activities are: Detecting Defects; Managing (and Preventing) System Problems; Recovering from System Problems; Implementing planned System Changes/Upgrades/Enhancements.</i>
		<b>Deliverables:</b> <i>System Changes/Upgrades/Enhancements</i>
		<b>Time Frames:</b> <i>As plan</i>
		<b>Who's Involved:</b> <i>System Owner, System User Representative, System/End Users, National Test Lab, National Configuration Management.</i>
3.1.3	IT Security Specialist implements and monitors the Project Disaster Recovery / Contingency Plan	<b>Purpose:</b> <i>A project Disaster Recovery/Contingency Plan activity must be tested and reviewed at a frequency commensurate with the risk level and expected magnitude of loss resulting from a service disruption. The IT Security Specialist is responsible for implementing this plan.</i>
		<b>Deliverables:</b>
		<b>Time Frames:</b>
		<b>Who's Involved:</b> <i>IT Security Specialist</i>

Number	Phase/Stage/Task	Process Description
3.1.4	IT Security Specialist perform recurring Security Certification / Accreditation	<b>Purpose:</b> <i>An major applications/system must be re-accredited whenever significant system changes occur and at least every three years.</i>
		<i>Security Certification must precede Security Accreditation. Security Certification is a formal statement, from the Designated Security Officer for the system, that the system meets its defined security requirements; is in compliance with all applicable policies and directives; and has reasonable security controls. Security Accreditation is the responsibility of the Business Process Owner and System Owner. The IT Security Specialist is responsible for performing Certification and Accreditation.</i>
		<b>Deliverables:</b>
		<b>Time Frames:</b>
3.1.5	System User Representative provides annual reports on both system performance and scope/schedule and budget information to the IMG	<b>Who's Involved:</b> <i>IT Security Specialist</i>
		<b>Purpose:</b> <i>As part of the Bureau's IT Portfolio, each system must provide information to the IMG (ITIB) so that the portfolio can be managed. Annual reporting would include scope, schedule and budget information for O&amp;M activities. Normal maintenance would be planned and funded as part of the system's annual operating costs.</i>
		<b>Deliverables:</b>
		<b>Time Frames:</b>
3.1.6	User Representative and Users establish mechanisms to plan and implement enhancements	<b>Who's Involved:</b> <i>System User Representative, AD's IRM Advisor (Portfolio Manager), System Owner and IMG.</i>
		<b>Purpose:</b>
		<b>Deliverables:</b>
		<b>Time Frames:</b>
3.1.6	User Representative and Users establish mechanisms to plan and implement enhancements	<b>Who's Involved:</b> <i>User Representative, Business Users, System Owner, CM, National Test Lab, SCO, and IMG</i>